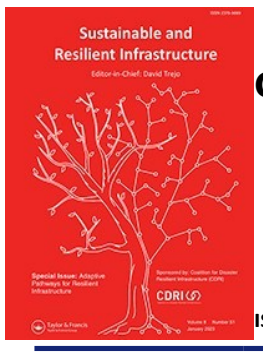
СТАЛА ТА СТІЙКА ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1, 85-101
https://doi.org/10.1080/23789689.2022.2128562



Стала та стійка інфраструктура

ISSN: (Print) (Online) Домашня сторінка журналу: https://www.tandfonline.com/loi/tsri20

З європейського досвіду захисту критичної інфраструктури до стійкості європейських критично важливих об'єктів: що це означає?

Крістер Пурсіайнен та Еерo Кютомаа

Щоб процитувати цю статтю: Крістер Пурсіайнен та Еерo Кютомаа (2023) "Від захисту європейської критичної інфраструктури до стійкості європейських критичних об'єктів: що це означає?", Стала та стійка інфраструктура, 8:sup1, 85-101, DOI: 10.1080/23789689.2022.2128562

Посилання на цю статтю: https://doi.org/10.1080/23789689.2022.2128562

СТАЛА ТА СТІЙКА ІНФРАСТРУКТУРА 2023, VOL. 8, NO. S1, 85-101
https://doi.org/10.1080/23789689.2022.2128562

Від захисту європейської критичної інфраструктури до стійкості європейських критично важливих підприємств: що це означає?

Крістер Пурсіайнена та Ееро Кютомаа

Факультет технологій і науки, кафедра технологій і безпеки, Арктичний університет Норвегії, Норвегія; Департамент національноїбезпеки, Міністерство внутрішніх справ, Фінляндія

АНОТАЦІЯ

Стаття є аналізом державної політики розвитку законодавства про критичну інфраструктуру в Європейському Союзі (ЄС), що охоплює 27 розвинених країн. Точніше, мова йде про Директиву CER 2022 року "Про стійкість критично важливих об'єктів". Ця директива прийшла на зміну Директиві ECI 2008 року "Про ідентифікацію та призначення об'єктів європейської критичної інфраструктури та оцінку необхідності поліпшення їхнього захисту". Ми запитуємо,що стоїть на кону в цьому процесі переходу від однієї директиви до іншої. Чому концепція захисту була замінена на концепцію стійкості, а концепція критичної інфраструктури - на новоявлену європейську концепцію "критично важливого об'єкта"? У заключному розділі ми обговорюємо євроінтеграційний в и м і р цієї нової директиви; що цей розвиток у сфері КІ говорить нам про поточну динаміку європейської інтеграції і як його можна пояснити?

ІСТОРІЯ СТАТТІ
Отримано 19 серпня 2022 року
Прийнято 15 вересня 2022 р.

КЛЮЧОВІ СЛОВА
Критична інфраструктура; стійкість; формування політики Європейського Союзу; повзуча інтеграція

Це аналіз розвитку законодавства Європейського Союзу (ЄС) щодо критичної інфраструктури (КІ) з точки зору державної політики, в якому висвітлюються зміни, обіцянки та виклики, що стоять перед ним. Це питання має очевидну важливість для 27 країн-членів ЄС, які є розвиненими високотехнологічними ринковими економіками і часто мають взаємопов'язану Критичну Інфраструктуру. Однак питання, що випливають з цієї перспективи, також становлять інтерес для країн за межами ЄС, оскільки всі країни мають вирішувати одні й ті ж проблеми: як підвищити стійкість **КІ**, а отже, і стійкість суспільств, в які вони вбудовані.

Питання є складним і багатогранним. З одного боку, воно стосується самої проблематики **КІ** з усіма її вимірами, секторами, суб'єктами і т.д., і, зокрема, концепції стійкості в цьому контексті. З іншого боку, вона заглиблюється в саму проблему європейської інтеграції. Питання стосується того, як розвиваються відносини між країнами-членами та ЄС навіть у такій сфері, яка, по суті, належить до мандату країн-членів. Директива CER свідчить про подальшу інтеграцію за межі вже існуючих наднаціональних сфер в ЄС.

Хоча **КІ** традиційно перебувала поза межами наднаціонального регулювання в ЄС, ситуація почала змінюватися близько п'ятнадцяти років тому. У 2008 році була прийнята так звана Директива ECI (Council of the European Union, 2008) "про ідентифікацію та призначення європейської критичної інфраструктури та оцінку необхідності її вдосконалення" (Council of the European Union, 2008).

"Захист" став першим обов'язковим до виконання регламентом Європейського Союзу у відповідній сфері. Він проклав шлях до нової сфери європейської інтеграції. У грудні 2020 року Європейська Комісія (2020a), спираючись на кілька середньострокових звітів і досить всеосяжний процес громадських слухань із зацікавленими сторонами, опублікувала свою пропозицію замінити Директиву ECI новою, відомою як Директива CER "про стійкість критично важливих об'єктів". Ця нова директива була остаточно затверджена у 2022 році.

Система ЄС з усіма її органами управління є досить складною. Щоб зробити її більш зрозумілою, часто кажуть, метафорично кажучи, що Європейський парламент (який представляє обраних на національному рівні партійних політиків) є своєрідною нижньою палатою. Європейська Рада (що представляє глав урядів або глав держав, які визначають загальний політичний напрямок і пріоритети) разом з Радою Європейського Союзу (що представляє галузевих міністрів держав-членів у різних сферах політики) складають верхню палату або сенат. Європейська Комісія є ініціатором та виконавчим урядом у сферах спільної політики. Згідно з процедурою прийняття директив ЄС, як і в нашому випадку (див. рис. 1), Європейська Комісія подала пропозицію у 2020 році, після чого шість профільних комітетів Європейського Парламенту належним чином обговорили її та надали свої детальні висновки. Поправки, запропоновані комітетами, розкривають більше приділення

КОНТАКТИ Крістер Пурсіайнен christer.h.pursiainen@uit.no

СТАЛА ТА СТІЙКА ІНФРАСТРУКТУРА 2023, VOL. 8, NO. S1, 85-101
https://doi.org/10.1080/23789689.2022.2128562

уваги самому процесу, ніж якимось серйозним розбіжностям, хоча деякі визначення були змінені, а також додані дрібніші питання. Після цього пропозиція пішла за типовою схемою з парламентськими читаннями, голосуванням, повторними читаннями, повторним голосуванням. Ця процедура була об'єднана в консенсусному проєкті звіту, а Європейський парламент згодом представив версію з узгодженими та запропонованими змінами (European Parliament, 2021a). Нарешті, формально організовані відповідно до стандартного регламенту, відбулися тристоронні переговори між Європейською Комісією, державами-членами, представленими в Раді у відповідній сфері (Рада з питань юстиції та внутрішніх справ), та Європейським Парламентом. Вони завершилися наприкінці червня 2022 року консенсусним рішенням щодо тексту директиви (Council of the European Union, 2022a). Зрештою, з'явилася нова Директива CER, яка має обов'язковий правовий статус для 27 держав-членів (Рада Європейського Союзу (2022b).

У цій статті ставиться питання про те, що стоїть на кону в цьому процесі переходу від однієї директиви до іншої. Чому концепція захисту була замінена на концепцію стійкості і чому концепція критичної інфраструктури була замінена новоявленою євро-концепцією критично важливих об'єктів (об'єктів критичної інфраструктури)? Що це за об'єкти і які сектори КІ вони представляють? Яка картина ризиків стоїть за новою **директивою**; хто або що загрожує європейській інфраструктурі? Чи є пріоритетними фізичні або кібернетичні ризики , або все разом, і як вони пов'язані між собою? Як нова директива реагує на той факт, що хоча держави-члени ЄС формально несуть відповідальність за захист своєї критичної інфраструктури, більшість з них перебувають у власності, управлінні та експлуатації приватних, а часто іноземних або транснаціональних компаній? Можливо, найважливіше, що в передостанньому розділі ми обговорюємо євроінтеграційний вимір цієї нової директиви; що вона говорить нам про поточну динаміку європейської інтеграції і як її можна пояснити?

У висновках ми виділяємо декілька проблем у чинній Директиві щодо СТВ, які слід зрозуміти та належним чином вирішити на ранній стадії. Це особливо важливо, коли 27 країн-членів ЄС починають впроваджувати досить далекосяжну і складну директиву в

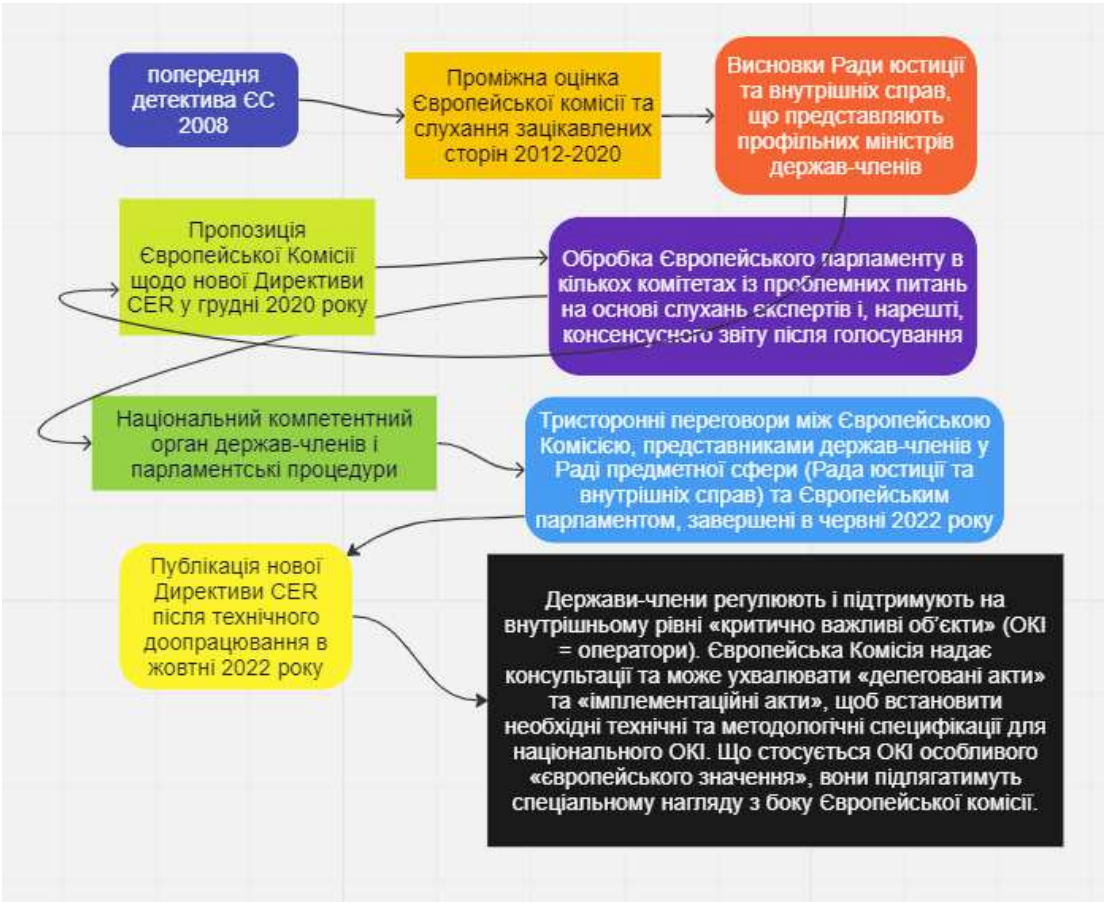


Рисунок 1. Політичний процес щодо директиви про ССВ.

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

контексті різних мов та адміністративних культур - щоб уникнути плутанини та непередбачуваних наслідків.

1. Методологічна записка

теоретичні засади

Ми поєднаємо вивчення типового документа державної політики з розглядом відповідних наукових досліджень щодо КІ та її стійкості. Оскільки це кабінетне дослідження зосереджується на розробці політики ЄС у сфері КІ, методологічний підхід полягає у структурованому порівнянні між попередньою Директивою про КІ (2008) та новою Директивою про ССВ (2022), а також політичними документами більш низького рівня. Цей порівняльний підхід має на меті визначити їх основні відмінності та подібності, а також основні тенденції розвитку.

Більш наукова література з питань КІ використовується для того, щоб проблематизувати і деконструювати основні припущення, закладені в описаних розробках. Хоча стаття не ставить за мету розвиток нової теорії, вона підсумовує основні наукові дебати в центральних сферах, які розглядаються в Директиві щодо ВК. Припущення полягає в тому, що політика ЄС зазнала значного впливу цих академічних досліджень, і в той же час ця політика відкриває нові напрямки досліджень або визначає їх пріоритетність.

Як зазначалося вище, потенційно більш глибоке теоретичне і політичне питання полягає в тому, чому країни-члени ЄС добровільно дозволили ЄС стати більш владним у регуляторному плані у сфері, яка належить до їхнього мандату і суверенітету. Таке питання є більш загальним політологічним питанням, яке також може бути застосоване до інших сфер досліджень європейської публічної політики, що виходять за межі нинішньої сфери комунікацій та інформації. З цією метою в кінці статті ми визначаємо три відомі школи теорії інтеграції, а саме: функціоналізм, підхід багатостороннього управління та теорію агентів і принципалів, які можуть бути застосовані до поточного питання і сприяти принаймні деяким теоретично обґрунтованим поясненням.

2. Чому стійкість і що вона означає?

Перше питання для обговорення - це зміна парадигми від захисту до стійкості у сфері КІ. З огляду на те, що "стійкість" за останнє десятиліття стала практично всеосяжною частиною наукового дискурсу та політичного жаргону, а також своєрідною панацеєю від усіх проблем, що ця зміна означає для організації ЄС?

2.1. Від захисту до стійкості

Коли Європейська Комісія почала приділяти увагу питанням КІ, зокрема, започаткувавши в середині 2000-х років Європейську програму захисту критичної інфраструктури (EPCIP) (European Commission, 2006a; див. підготовчі документи 2005, 2004), основна увага була зосереджена на захисті КІ (часто скорочено - CIP). Те саме стосується пропозиції щодо Директиви ECI (European Commission, 2006b) та пізнішої, доопрацьованої Директиви ECI (Council of the European Union, 2008). Хоча EPCIP визнає, що не всі об'єкти інфраструктури можуть бути захищені від усіх загроз, рішення полягало у визначенні пріоритетності окремих секторів КІ та набору загроз, від яких вони повинні бути захищені. Таким чином, питання здебільшого стосувалося традиційного управління ризиками з метою уникнення та запобігання небажаним подіям у певних секторах КІ.

Дійсно, ширша концепція стійкості взагалі не з'явилася в тогочасних політичних документах (Pursiainen, 2009, с. 727). В огляді Європейської Комісії (2012), присвяченому ЄІКЗІП, стійкість вже відігравала певну роль, хоча й невелику. Однак, як альтернативна концепція захисту, стійкість почала серйозно з'являтися в Європейській Комісії в контексті КІ приблизно до 2014 року (Pursiainen & Gattinesi, 2014). Тим часом концепція стійкості до КІ (іноді скорочено CIR) стала звичним явищем у більш наукових академічних дискусіях. У програмах фінансування досліджень ЄС "Горизонт 2020" та "Горизонт Європа", принаймні з 2014 року, конкурси, пов'язані з КІ, та відповідні затверджені проекти, по суті, стосуються не CIP, а CIR. Це призводить до розширення і поглиблення сфери досліджень.

Стійкість, у загальному розумінні, стосується "до, під час і після" небажаної події або порушення роботи КІ, таким чином,

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

охоплюючи весь цикл антикризового управління (Pursiainen, 2017). У контексті КІ це означає, що вона включає в себе докризовий захист - приділяючи увагу таким питанням, як надійність і здатність витримувати або протистояти стресу - але також припускає, що порушення в роботі КІ іноді неминуче відбуватимуться, і їх неможливо уникнути. Тому необхідно також посилювати абсорбційні та адаптаційні можливості, такі як резервування, а також стратегії відновлення (наприклад, Cantelmi та ін., 2021; Gritzalis та ін., 2019; Liu & Song, 2020; Mottahedi та ін., 2021; Rehak та ін., 2019; Rød та ін., 2020).

У проекті Директиви про СТВ 2020 року це питання вже належним чином відзначене, навіть є одним з основних а саме: "*необхідно докорінно змінити нинішній підхід із захисту конкретних активів на посилення стійкості критично важливих суб'єктів, які ними керують*" (European Commission, 2020a, с. 2, курсив додано). У цьому контексті "стійкість" означає здатність запобігати, протистояти, пом'якшувати, поглинати, пристосовуватися та відновлюватися після інциденту, який порушує або може порушити роботу критично важливого суб'єкта" (Європейська Комісія, 202a, стаття 2/2, с. 23). Насправді це досить добре відповідає основному визначенню в літературі з питань стійкості КІ. Зміна парадигми пояснюється, з одного боку, зростанням кількості держав-членів, які "дедалі більше усвідомлюють важливість мислення щодо стійкості, в якому захист є лише одним з елементів поряд із запобіганням та пом'якшенням ризиків, безперервністю бізнесу та відновленням" (European Commission, 2020a, с. 1). Більш формально, йдеться про рішення Ради ЄС від 2019 року, яке в основному стосується гібридних загроз, але включає розділ про КІ в цьому конкретному контексті зловмисних загроз; воно закликає Європейську комісію провести консультації з державами-членами щодо "пропозиції про перегляд Директиви [ECI] на початку нового законодавчого циклу, включаючи потенційні додаткові заходи для посилення захисту та стійкості критичної інфраструктури в ЄС" (Council, 2019, decision point 27). Виходячи з цього, Європейська Комісія у своїй пропозиції роком пізніше дійшла висновку, що необхідно забезпечити "більш комплексний підхід до забезпечення стійкості критично важливих об'єктів у низці секторів у всьому [Європейському] Союзі" (European Commission, 2020a, с. 5).

Що ж тоді являє собою цей "більш загальний підхід до стійкості критично важливих об'єктів" у Директиві CER? З академічної точки зору, нова пропозиція не зайшла дуже далеко. Щоправда, вона розрізняє "стійкість на рівні оператора та системну стійкість" (European Commission, 2020a, с. 5), але не зовсім зрозуміло, як саме слід визначати цю "системну стійкість". Однак для держав-членів сам перехід від захисту до стійкості має вирішальне значення, оскільки він змушує їх перебудовувати національні практики, правила і структури. Приблизно в той же період подібні зміни відбулисяі в НАТО, закріпивши таким чином зміну парадигми від захисту до стійкості практично в усій Західній Європі.

2.2. Як ми знаємо, що ІГС є стійкою?

Розширення сфери застосування концепції стійкості пов'язане з певними проблемами. Одна з головних проблем пов'язана з тим, як можна дізнатися, що КІ (або КЕ) є стійким. Яка наукова основа для оцінки або, можливо, навіть для вимірювання стійкості КІ?
Чим така оцінка стійкості відрізняється від традиційної оцінки ризиків?

Оцінка (або аналіз) *ризиків* та управління ними в цілому є добре дослідженою і навіть стандартизованою сферою (наприклад, ISO, 2018; ISO/IEC, 2019). Крім того, з 2013 року держави- члени ЄС вже зобов'язані проводити національну оцінку ризиків на основі законодавства Механізму цивільного захисту ЄС також включаючи сферу КІ, значною мірою спираючись на стандарти ISO (Pursiainen & Rød, 2021). На противагу цьому, не існує спільного, широко поширеного або стандартизованого розуміння того, як оцінювати та управляти *стійкістю* КІ. Це, власне, і є основним викликом для будь-якої політики та управління CIP або ССВ. А саме, перш ніж підвищувати стійкість, необхідно знати, наскільки стійкою наразі є КІ/ВК - і в яких сферах вона відстає від необхідного рівня стійкості - щоб підвищити стійкість в першу чергу.

Щоправда, в академічній сфері з'являється

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

все більше методологічної літератури про те, як вимірювати стійкість КІ (наприклад, AIIC, 2016; ANL, 2013; Gasser та ін., 2021; Hollnagel, 2017; Lee та ін., 2013; Linkov та ін., 2014; OECD, 2014; Panteli & Mancarella, 2017; Rehak та ін., 2019; Rød та ін., 2020; Sun та ін., 2020). У сфері КІ найбільш актуальними є **три сфери стійкості**, а саме: **суспільна, організаційна та технологічна**. Суспільна (або громадська) стійкість зосереджена на впливі порушень у сфері КІ на населення та життєво важливі соціальні функції постраждалої громади. Організаційна стійкість стосується впливу кризового управління на організаційному та міжорганізаційному рівнях, часто пов'язаного з такими питаннями, як готовність, раннє попередження, спроможність реагування, комунікація тощо. Технологічна стійкість більше стосується самого об'єкта, його надійності, адаптивності, надмірності, відновлюваності та здатності до відновлення. Відомий "трикутник стійкості" (популяризований Бруно та ін., 2003) зазвичай є базовою лінією для такого роду оцінок, спрямованих на зменшення трикутника в усіх його вимірах, що дозволяє довше витримувати стрес, швидше адаптуватися і швидше відновлюватися.

Ці сфери стійкості, очевидно, взаємопов'язані (у поєднанні з іншими сферами стійкості, наприклад, екологічною або психологічною). У більш методологічному сенсі можна виділити два підходи до оцінки стійкості. Моделювання та подальші симуляції дають змогу перевірити стійкість КІ з цифровими двійниками. Це може виявити деякі вузькі або слабкі місця в системі та допомогти у прийнятті рішень. Натомість системний підхід на основі індикаторів вимагає добре продуманого переліку індикаторів, субіндикаторів, їхніх вагових коефіцієнтів та алгоритмів для обчислення агрегованої стійкості. Іноді для цього розробляють програмні «інформаційні панелі» для створення "індексу стійкості", який слугує своєрідною метрикою стійкості КІ. Цей тип роботи є нескінченним і, по суті, схожий на управління ризиками, з тією різницею, що в ньому передбачається, що небажана подія вже відбулася. В обох випадках, як правило, численні невизначеності та взаємозалежності залишаються основною проблемою.

Однак за межами академічного світу питання оцінки або вимірювання стійкості КІ залишається недостатньо розробленим - або, скоріше,недостатньо стандартизованим. Зараз, у своїй пропозиції щодо Директиви про СВК, Європейська Комісія протягом усього документу пропонує, щоб СВК досягалася на основі оцінки ризиків. Цей підхід не був змінений в процесі розробки остаточного варіанту директиви. У довгостроковій перспективі це не є методологічно обґрунтованим. На відміну від оцінки та управління ризиками до події, що мають характер запобігання та пом'якшення наслідків, стійкість КІ також наголошує на готовності, реагуванні та швидкості відновлення, що застосовуються під час та після події. Іншими словами, на відміну від управління ризиками, передбачається, що небажані події та несподіванки можуть статися, оскільки запобігання та пом'якшення наслідків не завжди є достатніми(Park et al., 2013). Виклик тут полягає в тому, що якщо європейський регулятор вимагає від країн-членів CER або CIR, необхідно створити відносно спільне розуміння того, що означає стійкість у цьому контексті, як її можна оцінити і, виходячи з цього, як її можна підвищити, не обмежуючись лише традиційним управлінням ризиками. В іншому випадку всі країни-члени будуть робити це по-своєму, що призведе до різних варіантів імплементації нової директиви, а також суттєво вплине на обсяг відносних ресурсів, які виділяються на забезпечення стійкості КІ в країнах-членах.

Позитивною стороною цієї проблеми є те, що управління ризиками, яке вже значною мірою прийнято в галузі, може розглядатися як частина більш широкого управління стійкістю. Щоправда, деякі вчені розмежовують ризики та стійкість як досить антагоністичні напрямки і радять тримати їх окремо, щоб уникнути непродуманих інвестицій (Linkov et al., 2018). Інші ж пропонують єдиний підхід до ризикостійкості (Aven, 2019; Rød та ін., 2020). Ми дотримуємося останньої думки. Розумним підходом є зіставлення управління КІР з визначеннями та концепціями, які вже використовуються для управління ризиками, зокрема з міжнародними стандартами

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

сімейства ISO31000 (ISO, 2018; ISO/IEC, 2019). Перевага такого підходу полягає в тому, що оскільки багато організацій КІ вже знайомі зі стандартом, вони використовують його у своїй повсякденній роботі. Таким чином, можливе узгодження елементів стійкості з існуючими ризиками.

Вирішенням проблеми може стати широке поширення практики управління ризиками, а не пропозиція абсолютно нової схеми (Rød et al., 2020). Це вимагає як проактивних (запобігання та пом'якшення ризиків), так і реактивних (поглинання, адаптація та відновлення) підходів та можливостей для забезпечення стійкості.

Дійсно, під час процесу затвердження Директиви CER роль стандартизації була піднята, але не вирішена. Якщо ми не зможемо спільно визначити, як оцінювати стійкість КІ/КО, директива приречена на провал. Зміна парадигми від захисту до справжньої стійкості навряд чи буде реалізована на практиці, а лише створить хибне відчуття стійкості КІ.

При підготовці відповідного стандарту європейської організації зі стандартизації CEN/CENELEC або більш глобального стандарту ISO можна було б спиратися на такі максимуми, як: відсутність дублюючих практик; пристосованість; вимірюваність; відносна простота використання; і плюралізм методів оцінки (Rød et al., 2020). Останнє поняття "множинність" відповідає підходу до управління ризиками ISO 31000, який дозволяє використовувати будь-яку розроблену методику чи методологію оцінювання або їхні комбінації залежно від конкретних потреб і ресурсів, але при цьому слід визначати та дотримуватися основних принципів стандарту(див. ISO/IEC, 2019).

3. Що таке критичний суб'єктгосподарювання?

Як і у випадку з переходом "від захисту до стійкості", наступною зміною в пропозиції Європейської Комісії був перехід від концепції КІ до "критичного об'єкта", або КО. Отже, що таке критичний об'єкт у порівнянні з критичною інфраструктурою? Чи відображає це просто зміну лексики, чи передбачає щось більше? Ми вважаємо, що ця зміна може виглядати як незначна поправка до словника, але вона також вказує на своєрідну парадигмальну дилему. Ми вважаємо, що це тягне за собою перехід від секторів КІ до операторів КІ, що звужує рівень аналізу та дій.

Це також пов'язано з іншим питанням. А саме, Директива CER спрямована на підвищення стійкості "критичних об'єктів", які мають вирішальне значення для "підтримання життєво важливих суспільних функцій або економічної діяльності на внутрішньому [єдиному] ринку" (European Commission, 2020a, с. 4). Прив'язка КІ до внутрішнього ринку ЄС, що є основою європейської інтеграції, виводить картину на новий рівень аналізу, ширший, ніж суб'єкти та сектори. Внутрішній або єдиний ринок означає митний союз, який має спільну політику щодо регулювання продукції та свободи руху всіх факторів виробництва (товарів, послуг, капіталу та робочої сили). Крім того, наведена вище цитата також піднімає питання про те, що означають вищезгадані "життєво важливі суспільні функції".

3.1. Критичний суб'єкт господарювання - це оператор критичної інфраструктури, чи не так?

В одному з пунктів Директиви про ССВ (European Commission, 2020a, pp. 1.4.1, 38, курсив додано) згадуються "*оператори (які тут називаються "критично важливими суб'єктами")*". Належного обґрунтування цієї нової концепції не надано. Ймовірно, воно має на меті плавний перехід від секторів КІ (таких як енергетика) до більш конкретних операторів (таких як енергетична компанія) або, можливо, об'єктів (електростанція) для посилення та полегшення більш детального моніторингу та регулювання.

Однак досі не зрозуміло, чому не використовується широко вживане поняття "оператор КІ". Проблема з "новою євро мовою" очевидна. Якщо поглянути на різні офіційні переклади того, що означає "критичний суб'єкт" у різних мовних версіях Директиви CER (директиви перекладаються всіма офіційними мовами ЄС), то можна помітити, що, наприклад, у німецькій мові це *Einrichtung, що* приблизно відповідає англійському "facility"; фінською - *toimija,* що перекладається як "актор" або "агент"; італійською - *soggetto, що* означає "відповідальний суб'єкт"; шведською - *entitet, що в* цій мові, втім, по суті,означає якесь ціле; і так далі.

СТАЛА ТА СТІЙКА ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1, 85-101
https://doi.org/10.1080/23789689.2022.2128562

Тоді виникає питання, чи раціонально підібрана лексика. Чи може вона призвести до різних національних інтерпретацій і застосувань, особливо з огляду на складні структури приватної та державної власності національних КІ в різних комбінаціях? Це питання стає більш серйозним, оскільки нова директива обґрунтовується внутрішнім (або єдиним) ринком ЄС, що працює за єдиними правилами. Існує давня дискусія про те, що країни-члени ЄС по-різному виконують директиви ЄС, що пояснюється різними причинами, але, як правило, відображає відмінності в їхніх політико-адміністративних культурах (наприклад, Желязкова та ін., 2016). З іншого боку, стверджується, що ЄС нещодавно вдалося розробити нові інструменти для забезпечення дотримання та імплементації (наприклад, Börzel & Buzogány, 2019). Однак видається, що нечіткі концепції, відкриті для різних інтерпретацій, можуть негативно вплинути на дотримання вимог і тим самим посилити конкурентні позиції тих держав-членів, які визначають СІ більш вільно.

3.2. На словах говорити про життєво важливі суспільні функції як про дедуктивний підхід?

Можливо, більш важливим питанням є те, що є тими "життєво важливими суспільними функціями", які згадуються як критичні для внутрішнього (або єдиного) ринку? Ще у 2012 році в доповіді у попередній самооцінці EPCIP, проведеній Європейською Комісією (2012), було висловлено думку, що низка країн-членів дотримується "системно-орієнтованих національних програм CIP, кінцевою метою яких є безпека і стійкість систем, що може включати діяльність у різних секторах". Це стосується як "системної стійкості" між критично важливими системами, так і того факту, що не слід обмежуватися лише об'єктами.

Дійсно, розуміння життєво важливих/критичних суспільних функцій, що є ширшим, ніж просто інфраструктура, завжди було прийнято фактично кількома державами-членами, особливо в Північній Європі (див. Pursiainen, 2018, с. 633-634). Для прикладу такого підходу, наприклад, норвезька система (яка не є частиною ЄС, але входить до Європейського економічного простору (ЄЕП), а отже, тісно пов'язана з ЄС у всіх аспектах) починається з "суспільних потреб", які охоплюються "життєво важливими або критичноважливими суспільними функціями". Останні залежать від "інфраструктури", критичність якої оцінюється через "надійність", "альтернативи" або надмірність та "тісний зв'язок". Ця оцінка формує основу для прийняття рішення про те, чи є певна інфраструктура критичною або некритичною (NOU, 2006). Такими базовими потребами можуть бути, наприклад, "керованість і суверенітет", "безпека населення" та "суспільна функціональність". Вони, у свою чергу, можуть бути поділені на підкатегорії життєво важливих суспільних функцій, таких як державне управління, електропостачання, продовольча безпека, послуги з надзвичайних ситуацій тощо (DSB, 2017).

Зараз, схоже, Європейська Комісія вирішила охопити життєво важливі суспільні функції, критичні сектори інфраструктури та об'єкти критичної інфраструктури в одному пакеті. Проблема полягає в тому, що одиницею або рівнем аналізу нової директиви є критичний суб'єкт, а саме оператор, а не життєво важливі суспільні (та економічні) функції. Таким чином, він використовує індуктивний, висхідний або агентний підхід. Ми не стверджуємо, що ці різні рівні є антагоністичними. Але ми стверджуємо, що такий законодавчий підхід ускладнює розмежування критичної інфраструктури від некритичної, оскільки не існує чіткої методології щодо того, що таке об'єкт і за яких умов він є критичним. Зокрема, за визначенням, стійка система повинна мати певну надлишковість, і не слід надто покладатися на критичність будь-якого об'єкта чи оператора. З точки зору суспільства, цей концептуальний і парадигмальний вибір, що переходить від окремих об'єктів КІ до життєво важливих суспільних функцій, дозволить застосувати підхід, більш орієнтований на забезпечення стійкості, ніж той, що пропонується Директивою CER.

4. Підвищення критичності до всього?

Проблема політики ЄС у сфері комунікацій та інформації з самого початку полягала в тому, як провести межу між ЄС, компетенції ЄС та країн-членів. Варто

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

нагадати, що ця сфера в основному все ще належить до мандату останніх, але тепер, коли Директива про CER пов'язує європейський CER з внутрішнім ринком ЄС, він за визначенням стане більш європейським з точки зору мандату. Це, в свою чергу, призводить до питання про те, що являє собою КІ/КО, і які з численних КІ можна розуміти як європейські КІ (або ЕКІ), або такі критичні суб'єкти, що підпадають під дію нової Директиви про СЄР.

4.1. Скільки секторів є критичноважливими для Європи?

Питання про те, які сектори КІ слід вважати європейськими, досить довго обговорювалося під час підготовки Директиви про ІКІ 2008 року. Обговорювалося навіть питання, чи може ІКЦ розташовуватися за межами Європи, якщо він впливає на ЄС. Ця дискусія незабаром була закрита. Європейська Комісія (2006b, Додаток 1, с. 21) спочатку запропонувала одинадцять секторів КІ та двадцять дев'ять підсекторів КІ. У процесі обговорення проекту Директиви про КІ в Європейському Парламенті пропонувалося все більше і більше додаткових секторів. Це, очевидно, занепокоїло деякі держави-члени, які побачили загрозу своєму суверенітету в сфері КІ. Тому в остаточно схваленій Директиві 2008 року *лише два сектори* - енергетика і транспорт - були визнані "європейськими", а потім деталізовані і поділені на вісім підсекторів (Рада Європейського Союзу, 2008, L 345/75 і Додаток 1, с. L 345/81). Це двосекторне рішення було ще більше обмежене інфраструктурою, розташованою в державах- членах, де перебої в роботі мали б значний вплив щонайменше на дві інші держави-члени. Обговорювалося багато варіантів того, скільки країн-членів повинно бути задіяно, але їх стало дві. У наступні роки інформаційно-комунікаційні технології (ІКТ) часто згадувалися як можливий новий сектор КІ, який можна було б додати до переліку ЄКІ, оскільки вони вважалися горизонтальним сектором КІ.

Наразі, значне розширення європейського регулювання в частині секторів ІК охоплюється Директивою про ССВ. За пропозицією Європейської Комісії, вона включає десять секторів, а саме: енергетику, транспорт, банківську справу, інфраструктуру фінансових ринків, охорону здоров'я, питну воду, водовідведення, цифрову інфраструктуру, державне управління та космос (European Commission, 2020a, с. 3). Для того, щоб зробити відповідні директиви більш сумісними, ці сектори навмисно ті самі, що й у запропонованій одночасно Директиві з кібербезпеки NIS2 (European Commission, 2020c).

4.2. Взаємозалежності та система систем

Проблема полягає в тому, як визначити «критичні об’єкти» у цих «секторах критичної інфраструктури». Директива CER фундаментально базується на ширшому виклику залежностей і взаємозалежностей. Вони стосуються принаймні трьох різних типів взаємозв’язків, а саме між різними секторами, між країнами та між фізично-цифровими інтерфейсами. Однак це стає ще складнішим, коли ми фактично обговорюємо «системну стійкість» CER у тому сенсі, як це описано в пропозиції Європейської Комісії; або «система систем», як її зазвичай називають у літературі КІ. У принципі, весь ланцюжок поставок будь-якого сектора критичної інфраструктури належним чином стає критичним, включаючи не лише інші сектори КІ чи критичні об’єкти, а й, здавалося б, некритичні сектори чи об’єкти. Тоді це пов’язано з так званими «відомими невідомими», а саме «сутностями», про існування яких ми знаємо, але не знаємо, що вони є критичними до того, як настане криза. Як зазначалося вище, у пояснювальному розділі Європейської комісії (2020a, стор. 5), але не в самому тексті директиви, проводиться різниця між «стійкістю на рівні оператора та системною стійкістю». Хоча перші ризики легко зрозуміти, що ж тоді таке «системні ризики» в контексті КІ? Директивна пропозиція та схвалена директива не розкривають це детальніше, але ми отримуємо натяк із конкурсів ЄС Horizon Europe на 2021–2022 роки (керованих Європейською Комісією), які були відновлені для надання наукової підтримки реалізації нової політики ЄС (Європейська комісія, 2021a, стор. 96–112). Схоже, що увага зосереджена на стійкості до «різних очікуваних і несподіваних подій, нових ризиків, будь то природні чи створені людиною, ненавмисні, випадкові чи зі злим умислом». Ці ризики є системними через їх

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

«системний вимір і складність атак і збоїв за допомогою кібернетичних або фізичних засобів», включаючи взаємозалежності в межах кількох типів інфраструктури та через їхній транскордонний вплив. Академічний план-підхід до розуміння взаємозалежностей КІ вже був представлений на початку 2001 року (Rinaldi та ін., 2001). З точки зору практичного управління взаємозалежностями, проблема полягає в тому, що коли критичні системи об'єднуються разом, критичні елементи кожної стають критичними елементами всіх через можливість того, що збій в одній частині однієї системи буде передано іншим. Таким чином, дилема системи систем полягає в тому, що оператори КІ («суб'єкти») зазвичай знають і ефективно контролюють ризики своєї власної системи, але не ризики інших систем, від яких вони залежать. Уже існує безліч теоретизацій, моделювання та моделювання в галузі розробки надійності та стійкості, які показують, що несподівані взаємозалежності часто виникають або можуть мати місце. Якщо взяти до уваги цю інформацію, можна змоделювати найкращі стратегії відновлення для взаємозалежних КІ (наприклад, Eusgeld та ін., 2011; Ouyang & Wang, 2015; Thacker та ін., 2017). Однак існує не так багато емпіричних доказів реальних збоїв КІ, які були б спричинені залежностями чи взаємозалежностями між різними об'єктами чи секторами КІ. Це ставить питання про те, що ми знаємо про взаємозалежності; відповідь полягає в тому, що ми багато чого не знаємо. Проте з точки зору концептуалізації взаємозалежностей були запропоновані корисні типології. Якщо операції залежать від матеріального результату(ів) іншої інфраструктури через функціональний і структурний зв'язок між входами та результатами двох активів, вони вважаються фізичними. Якщо операції залежать від інформації та даних, що передаються через інформаційну інфраструктуру через електронні або інформаційні канали, вони вважаються кібер. Якщо операції залежать від локального середовища, де подія може викликати зміни в стані операцій у кількох інфраструктурах, їх називають географічними. І якщо операції залежать від стану іншої інфраструктури через зв'язки, відмінні від фізичних, кібернетичних чи географічних, вони вважаються логічними, оскільки такий вид (взаємо)залежності можна віднести до людських рішень і дій, та не є результатом фізичних операцій чи кіберпроцесів (наприклад, Petit et al., 2018). Але чи є КІ залежними чи взаємозалежними? Залежність – це зв'язок між двома критично важливими продуктами чи послугами, у яких один продукт чи послуга необхідний для створення іншого продукту чи послуги. Залежність = взаємозалежність. Однак бракує європейських міжгалузевих або транскордонних баз даних про збої КІ та відповідних наукових досліджень. Проте деякі дослідження (Luiijf & Klaver, 2021; Luiijf et al., 2009) показують, що близько третини зареєстрованих переважно національних інцидентів у Європі є наслідком інцидентів в інших службах. Сектори енергетики (особливо електроенергії) та ІКТ.

4.3. Штучний інтелект може допомогти, але може також ускладнити.

Нібито підхід штучного інтелекту (ШІ) розвивається в рамках відповідних досліджень не лише для моделювання та імітації взаємозв'язків між системами, але й для аналізу, прогнозування та підтримки прийняття рішень для операторів КІ. ШІ спрямований на заміну або доповнення людських суджень і дій. Багато в чому ШІ буде корисним, автоматизуючи роботу КІ і навіть виявляючи кібератаки та подібні небажані події та реагуючи на них (наприклад, Begli et al., 2019; Kumar & Choi, 2022). Вважається, що штучний інтелект та інші новітні технології (цифрові близнюки, Інтернет-складових тощо) необхідні особливо для вирішення надзвичайних ситуацій КІ, спричинених зміною клімату, які важко передбачити або керувати ними лише за допомогою управління ризиками та інспекцій (Argyroudis et al. ін., 2022). Наголошується, що для цього необхідна відповідна стандартизація. Проте очевидно, що якщо штучний інтелект використовується для оцінки потенційних ризиків, виявлення загроз у реальному часі та надання варіантів прийняття рішень для КІ або навіть для прийняття рішень дещо поза контролем людини, це відкриває нові шляхи для зловмисних кібератак на вхідні дані. а також вихідні дані та алгоритми ШІ, що керують КІ (наприклад, Laplante & Amaba, 2021; Khurana та ін., 2019). З іншого боку, штучний інтелект також може використовуватися, і вже використовувався, для створення складних кібератів (наприклад, Kaloudi & Li, 2020). Щоправда, органи ЄС добре усвідомлюють цю загрозу, якщо ще не готові до неї. Належний закон про штучний інтелект, запропонований Європейською комісією (2021b), проходить через Європейський парламент і Раду для запровадження регуляторного контролю до цього поля. Запропонований Закон про

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

штучний інтелект містить перелік систем штучного інтелекту високого ризику, які включають: «Управління та експлуатація критичної інфраструктури: (a) системи штучного інтелекту, призначені для використання в якості компонентів безпеки в управлінні та експлуатації дорожнього руху та постачанні води, газу, опалення та електроенергії» (Європейська Комісія, 2021c, Додаток II, 2a). Кілька інших менш фізичних систем, які можна розглядати як частину КІ, також згадуються в інших підзаголовках систем штучного інтелекту високого ризику, таких як правоохоронні органи, прикордонний контроль і система правосуддя. Ці системи мають свої особливі вимоги (Європейська комісія, 2021c, розділ 2), що стосуються, наприклад, таких питань, як управління ризиками, управління даними, технічна документація, точність, стійкість та кібербезпека. Однак, як можна собі уявити, на основі поточного досвіду постійно розвиваються кіберзагроз, і сам факт того, що КІ став повністю інтегрованим, кіберфізичні системи (так звані CPS), хакери, терористи, злочинці та особливо зловмисні іноземні держави неминуче з'являться, щоб скористатися вразливістю та нанесенням ймовірної шкоди які можуть бути спричинені націлюванням на системи AI CI, а також створенням шкідливих технологій AI для CI.

5. Еволюція ландшафту ризиків

При підготовці Директиви ECI 2008 р. вибір між тероризмом або підходом, що передбачає всі небезпеки, був одним із головних питань (Pursiainen, 2009, стор. 730–732). Це було пов'язано з тим, що в США, а отже, і в НАТО, новий інтерес до захисту КІ був прямим наслідком атак 11 вересня. Вибухи в приміських потягах у Мадриді 2004 року та терористичні атаки на метро в Лондоні 2005 року безумовно змінили увагу майбутнього EPCIP на тероризм. Це призвело до упередженого розуміння причин збоїв КІ. Отже, як цю ситуацію визначає Директива CER?

5.1. Від тероризму як пріоритету до підходу, що враховує всі небезпеки.

Рішення делегувати питання КІ тодішньому Генеральному директорату (DG) Home в Європейській Комісії замість Генерального директорату, який відповідає за цивільний захист, частково відображає цей акцент на тероризм. У той же час, у державах-членах відповідний компетентний орган цілком може бути тим, хто займається звичайними питаннями цивільного захисту. Здавалося б, було досягнуто певного компромісу під час формулювання остаточної Директиви 2008 року про раннє втручання; це посилається на попередній заклик Ради юстиції та внутрішніх справ від грудня 2005 року до Європейської комісії підготувати EPCIP відповідно до підходу, згідно з яким «техногенні, технологічні загрози та природні катаклізми повинні бути прийняті до уваги в процесі захисту критичної інфраструктури, але загрозі тероризму слід надати пріоритет» (Рада Європейського Союзу, 2008, L 345/75, курсив додано). Здається, неявну напругу між тероризмом і зосередженістю на всіх небезпеках у попередньому підході було якщо не повністю вирішено, то принаймні краще зрозуміло, а підходи краще узгоджено. Це частково тому, що концепція гібридних загроз входила в картину, яка, в той же час, служила для подальшого ускладнення ландшафту ризиків. У новій Директиві CER підхід, що базується на всіх небезпеках, тепер буквально прийнятий, хоча це було виправдано зміною «середовища, в якому діють критичні суб'єкти», а також тим фактом, що «ландшафт ризиків є складнішим, ніж у 2008 році» (Європейська комісія, 2020a, с. 2). Таким чином, це включає природні небезпеки, спонсоровані державою гібридні дії, тероризм, внутрішні загрози, пандемії та великі аварії в поєднанні з проблемами, які створюють нові технології, такі як 5G або безпілотні транспортні засоби, з точки зору вразливості. Тема секторальних взаємозалежностей і каскадних ефектів також сильно передається. Дуже пов'язане питання та своєрідна змінна полягає в тому, чи слід європейській політиці зосереджуватися переважно на фізичних загрозах, чи вони також повинні приділяти увагу кіберзагрозам. У ранній європейській (а також американській) політиці кіберзагрози зазвичай обговорювалися як окремий CII, тобто захист критичної інформаційної інфраструктури, а не частина політики CI (Pursiainen, 2009, стор. 728–730). Спочатку рішення полягало в тому, щоб зосередитися на обох, але на практиці інтеграція фізичних загроз і загроз кібербезпеці була лише в зародковому стані під час підготовки Директиви ECI у 2008 році, і ці дві сфери захисту КІ залишалися досить відокремленими. Пропозиція CER, а згодом і Директиви, здається, добре узгоджені на загальному рівні з директивами з кібербезпеки (NIS, NIS2). У 2016 році було запропоновано замінити тоді ще досить нову NIS (Рада Європейського Союзу, 2016) всього через чотири роки на NIS2 (Європейська комісія,

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

2020b). Це значною мірою було виправдано швидкою цифровізацією внутрішнього (єдиного) ринку та інших видів діяльності через Covid-19. Пропозиція NIS2 була опублікована в той самий день, що й нова пропозиція Директиви CER, яка, здавалося б, утворює взаємопов'язаний пакет європейського законодавства. Однак чим складнішою стає картина загроз, тим важче визначити належні стратегії стійкості для КІ. Окрім обліку незалежних небезпек, необхідно також розробити стійкі, абсорбційні, адаптивні та відновлювальні моделі та стратегії для більш складного контексту багатьох небезпек, де кібератаки, стихійні лиха, пандемії та антропогенні небезпеки потенційно можуть відбуватися одночасно в різних комбінаціях та динаміці. (Argyroudis та ін., 2020). Оскільки всі небезпеки або їх комбінації неможливо спрогнозувати, підготувати до них або навіть змоделювати, дослідники кризового менеджменту поспішили зауважити, що складно розробити єдиний план готовності, який охоплює всі потенційні виклики, що виникають у кризових ситуаціях. Таким чином, планування на випадок надзвичайних ситуацій насправді має стосуватися планування того, як імпровізувати. Отже, повинні бути доступні як проактивні (заздалегідь), так і реактивні (коли настане криза) стратегії стійкості. У будь-якому випадку, планування не повинно бути занадто жорстким і не повинно створювати перешкоди для імпровізації (McConnell & Drennan, 2006; Stern, 2013).

5.2. Гібрид ризикує ще більше ускладнює проблему

Хоча такі явища, як зміна клімату та нові технології, іноді призводять до неочікуваних або нових ризиків, у Директиві CER також наголошується на особливій категорії ризику, а саме зловмисних гібридних загрозах. Однак у ньому не йдеться про ці загрози. У попередніх політичних документах на цей рахунок (Рада Європейського Союзу, 2019) гібридні загрози зазвичай включають, наприклад, кібератаки, зловмисні прямі іноземні інвестиції, дезінформацію та автоматизовані транспортні засоби – усі вони можуть бути інструментами зловмисних дій проти Європейська інфраструктура. Видання 2020 року «Огляду ризиків природних і техногенних катастроф, з якими може зіткнутися Європейський Союз» (Європейська комісія, 2021d, наприклад, стор. 130) надає дещо детальнішу картину зловмисної гібридної стратегії, яка може поєднувати фізичні та кібератаки з кампанії з дезінформації, зміна структури власності або розгортання компонентів з іноземних джерел. Це породжує проблему, пов'язану з тим, що багато з вищезазначених елементів гібридних загроз – гібридних у тому сенсі, що вони застосовуватимуться одночасно або в каскадному режимі в різноманітних комбінаціях – поза межами досяжності жодної «критично важливої сутності». Зокрема, це передбачало б добре скоординовану міжгалузеву та багатонаціональну оперативну співпрацю, можливо, у поєднанні з ШІ. Таким чином, практичне питання полягає в тому, як держава-член, віддана ліберальним цінностям, координує захист від гібридних загроз, пов'язаних із КІ, не порушуючи головних принципів цього ринкового лібералізму шляхом створення якогось багатогалузевого оперативного органу або «критично важливої організації» для управління кризами. . Це природно призводить до обговорення державно-приватного партнерства чи інших багаторівневих моделей управління.

6. Державно-приватне партнерство або більше регулювання?

У той час як уряди вважаються відповідальними за захист КІ в контексті ЄС, більша частина цих КІ все більше належить, адмініструється та управляється приватним сектором. Урядам просто не вистачає монополізованих повноважень, знань і ресурсів, щоб реально виконати обов'язки щодо забезпечення стійкості своїх КІ. Це ще більше ускладнюється інколи багатонаціональними або іноземними структурами власності секторів КІ. Отже, якою буде ситуація після нової Директиви CER?

6.1. Держави-члени регулюють

Це питання з самого початку було викликом для європейської політики КІ. В основному, альтернативи полягають у додаванні регулювання, або саморегулюванні компаній КІ, щоб уникнути державного регулювання, або в якійсь комбінації в термінах ідеалізованого державно-приватного партнерства (ДПП).

Як компанії, які прагнуть отримати прибуток у переважно конкурентному бізнес-середовищі, малоймовірно, що сектори КІ, оператори чи організації будуть саморегулюватися більше, ніж це було суворо необхідно. Логіка Директиви CER полягає в тому, що вона регулює країни-члени, а країни-члени зобов'язані регулювати свої КО/КІ. Але що передбачає це регулювання з точки зору ДПП? Директива CER, здається,

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

означає крок до більшого регулювання, хоча в основному делеговано державам-членам. Найбільш помітно це представлено в статтях 9–19 Директиви CER, таким чином охоплюючи більше третини з 26 статей директиви. Це свідчить про значне збільшення уваги до регулювання, хоча повідомлення не зовсім чітке. Регулювання сформульоване в дусі того, що регулювання з боку держави насправді є «підтримкою» приватних або державних компаній, які керують КІ. *Очікується, що уряд країни-члена надасть таку підтримку критично важливим суб'єктам у формі матеріалів, методологій та навчання, щоб забезпечити їх стійкість*. Проте виглядає дещо сумнівним те, чи мають уряди такі можливості та спроможності, якщо вони не почнуть значно покращувати свої національні дослідження КІ та таким чином працювати через академічну та дослідницьку спільноту. Також очікується добровільний обмін інформацією між компетентними державними органами та РЄ. Цілком ймовірно, що це як таке стане не чим іншим, як продовженням попереднього ДПП, якщо воно колись спрацює ефективно. Однак Директива CER також вимагає, щоб держава-член ідентифікувала конкретні об'єкти КІ, які підпадають під дію Директиви CER, для кожного сектора та підсектору КІ. Це може бути важким завданням і приреченим на свавілля без будь-яких чітких критеріїв. Проте перелік цих об'єктів ЄКІ має бути наданий Європейській комісії, і кожен такий ЄКІ буде повідомлено про їх ідентифікацію як ЄКІ, з їхніми відповідними зобов'язаннями регулярно оцінювати свої ризики на основі національних оцінок ризиків, а потім, у добре задокументованим способом «вжити належних і пропорційних технічних і організаційних заходів для забезпечення їх стійкості». Очевидно, що це тягар, що регулюється державою, для ЄКІ, але також і для державних органів, оскільки вони мають оптимізувати цей вид національного регулювання ЄКІ. Навіть більш складним завданням є те, як упорядкувати підходи держав-членів.

6.2. Або Єврокомісія регулює?

Яка тоді роль Європейської комісії в цьому процесі після схвалення директиви? Є певні ознаки того, що національні КІ підлягають зовнішньому оцінюванню не лише державами-членами. На запрошення держав-членів консультативні місії організовані Європейською Комісією, мають надати консультації КІ щодо виконання їхніх зобов'язань. Крім того, Європейська Комісія уповноважена приймати «делеговані акти» та «імплементаційні акти» з метою встановлення необхідних технічних і методологічних специфікацій для національного КІ. Коли справа доходить до КІ «особливого європейського значення», вони підлягатимуть спеціальному нагляду з боку Європейської комісії. Оскільки незрозуміло, як буде виглядати ця нова практика регулювання і в яких випадках вона буде застосовуватися, перші практичні досвіди цієї нової практики ще належить побачити. Тоді як на практиці Європейська Комісія може мати достатні знання, щоб підтримувати та консультувати держави-члени щодо таких досить складних і часто технологічних питань? Дійсно, вона цілком може мати такий досвід. Слід згадати, наприклад, значне сприяння ЄС дослідженням, розробкам та інноваціям (RDI), зокрема Horizon Europe, багатосотмільярдній програмі, яка проводить регулярні великомасштабні конкурси, пов'язані з КІ (Європейська комісія, 2021a).). Конкретно кажучи, проекти окремо або разом створюють практичні рекомендації, які часто перевіряються в реальному КІ та досягають високого рівня технологічної готовності (TRL), як перевірено на практиці. У той час як учасниками проектів є окремі дослідницькі установи, оператори КІ та компетентні органи, Європейська Комісія в основному визначає порядок денний і фасилітує дослідження, пов'язані з політикою ЄС, і політичні поради. Ще однією платформою, про яку варто згадати, є власна служба науки та знань Європейської комісії, Об'єднаний дослідницький центр (JRC), який об'єднує тисячі дослідників у кількох країнах у майже всіх галузях. У сфері СІ вона включає, наприклад, Європейську довідкову мережу захисту критичної інфраструктури (ERNCIP, n.d.). Робота ERNCIP організована в тематичних групах (наприклад, авіація, промислові автоматизовані системи управління), які об'єднують сотні учасників, які є експертами з держав-членів, які працюють у промисловості, наукових колах або компетентних органах.

7. Повзуча інтеграція або раціональний поділ праці?

Наведене вище обговорення неминуче спонукає нас до роздумів над цим питанням у значно ширшому контексті європейської інтеграції та її динаміки. Чим можна пояснити той факт, що країни-члени, здавалося б, добровільно, і протягом останніх п'ятнадцяти років дедалі частіше, обмежили свій суверенітет у сфері, яка в

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

принципі не є наднаціональною?

7.1. Не індивідуальна робота, але нестандартна?

Слід зазначити, що зростання ролі Європейського Союзу в сфері політики та регулювання КІ не є нетиповою подією. Це відбувається і в інших сферах, де Єврокомісія не має чіткої наднаціональної влади. Це можна зрозуміти як тенденцію до того, що було названо «повзучою компетентністю» або «неформальним управлінням». До таких галузей належать, зокрема, навколишнє середовище, регіональний розвиток, дослідження та технологічний розвиток, енергетика, цивільна безпека, спільна зовнішня політика та політика безпеки та політика охорони здоров'я (наприклад, Pursiainen & Rød, 2021; Bergmann, 2019). ; Greer & Löblová, 2017; Riddervold, 2016; Riddervold & Rosén, 2016; Princen, 2016; Kirchner et al., 2015; Maltby, 2013; Princen & Rhinard, 2006; Christiansen et al., 2004; Pollack, 1994, 2000). Тим не менш, Директива CER була підготовлена належним чином демократичним і прозорим способом. Поточне рішення було обрано, оскільки національні компетентні органи, і навіть оператори КІ, які представляють різні сектори, здавалося, підтримали або навіть запропонували його в попередньому процесі оцінювання (Європейська Комісія, 2019). Остаточна директива, природно, також забезпечується державами-членами та Європейським парламентом у належному та детальному процесі. Усі ці процеси та відповідні органи добровільно передають певні повноваження щодо регулювання, визначення порядку денного та прийняття рішень з національного на міжнаціональний рівень, що на практиці означає Європейську комісію. Так чим це пояснюється?

7.2. Раціоналістична інтеграція?

Здається, ця розробка підтримує (принаймні) три певною мірою взаємопов'язані «теоретичні школи», прикладом яких є дослідження європейської інтеграції. З точки зору традиційного «функціоналістського» підходу (Haas, 1958) або його переглянутої «неофункціональної» версії (Haas, 1964, 1990; Schmitter, 2005), держави добровільно призначають деякі обов'язки експертного рівня, контроль, і повноваження наднаціональної влади в ім'я їхніх функціоналістичних потреб; речі повинні бути зроблені. У нашому випадку це цілком може відображати логіку національних компетентних органів, які протягом п'ятнадцяти років роботи з цим питанням у контексті попередньої Директиви ECI від 2008 року дійшли висновку, що більш централізований підхід , для захисту національних КІ було необхідно ефективне та ширше регулювання ЄС. Хоча Рада (представляє країни-члени) та Європейський парламент (представляє обраних на національному рівні партійних політиків), ймовірно, покладаються не лише на свою ідеологію, але й значною мірою на погляди експертів і лобістів, їхній позитивний підхід, можливо, можна додатково зрозуміти з точки зору зростаючої напруги між супердержавами ззовні. Зокрема, йдеться про гібридні загрози з боку Росії та Китаю. Країни-члени розуміють, що їх стійкість до КІ краще врегулювати в межах ЄС, що зокрема вони діють ізольовано. Вищезазначене функціоналістське пояснення включає деякі припущення щодо конвергентних систем переконань відповідних учасників. Але це в основному раціоналізм. Запровадження аргументу ефективності внутрішнього (або єдиного) ринку в цьому контексті для виправдання посилення європейського регулювання не здається доречним приводом. Це скоріше реальний наслідок посилення взаємозв'язку європейських країн або зусиль захистити цей взаємозв'язок від зовнішніх, зловмисних гібридних та кіберзагроз, на додаток до таких питань, як непередбачувані небезпеки, спричинені зміною клімату, які стають дедалі більшими. частішими і важчими. Говорячи більш сучасними теоретичними термінами, поточну справу також можна розглядати як приклад європейського «багаторівневого управління» (Tömmel & Verdun, 2009), або гібридної системи управління, де ЄС рано чи пізно покриває майже всі сфери політики. Це відбувається або через формальну компетенцію, або, як у нашому випадку, через досить м'яку координацію та сприяння. Тоді наш випадок можна пояснити твердженням, що структура управління має відображати ефективне виробництво суспільного блага (стійкість європейської КІ) та/або що управління має принаймні відображати моделі спільноти (ЄС), де воно має місце (Schakel та ін., 2015). Крім того, описаний вище розвиток відображає логіку відомої «теорії принципала-агента» (De la Porte, 2011; Pollack, 2003). Уряди (принципал) делегують свої повноваження Європейській комісії (агент) через асиметрію інформації та ресурсів, при цьому остання може отримати кращий огляд ризиків КІ на європейському рівні та способів скоординованого управління ними. Спільним для

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

всіх вищезазначених теоретичних шкіл є те, що вони пояснювали б розвиток політики ЄС щодо КІ, наголошуючи на логічній інтеграції політики в країнах-однодумцях, які в основному мають однакові інтереси, у контексті дедалі більшого внутрішнього виклику. Зовнішні виклики, пов'язані із взаємозв'язками, залежностями та взаємозалежностями.

8. Висновки: проблеми ввпровадження

На завершення окреслимо кілька викликів на основі наведеного вище аналізу, зокрема тих, які пов'язані з імплементацією досить складної Директиви CER у 27 країнах з різними мовами та політико-адміністративною культурою в контексті багаторівневого управління державами-членами ЄС. . **Проблема 1.** У цій статті обговорювалася парадигматична зміна європейської політики КІ від захисту до ширшої концепції стійкості. Сам процес певною мірою визнав збій підходу захисту. Таким чином, слід приділяти більше уваги адаптивності та відновленню щодо порушення КІ. Однак це також викликало питання про те, як ми можемо знати, чи є певний об'єкт КІ або відповідний сектор КІ стійким. Питання в тому, що без спільного узгодження або стандартизованих способів його оцінки або вимірювання, всі країни-члени розроблять власні рішення. Таким чином, ми пропонуємо стандартизацію певного базового рівня оцінки стійкості КІ. **Завдання 2**. Нашу трохи критичну увагу привернуло введення нового терміну «критичний суб'єкт» до поточної теми. Європейська комісія пояснює, що це еквівалентно оператору КІ. Це як таке означає, що концепція СЕ не приносить багато інновацій у сферу. Він скоріше плутає регулятивну лексику з різними національними перекладами. З іншого боку, це, здається, вказує на переміщення уваги від секторів КІ до рівня конкретних об'єктів КІ, операторів чи організацій, без чіткого формулювання цього як такого. Таким чином, він лише на словах приділяє увагу підходам, які більше зосереджуються на життєво важливих суспільних функціях. Директива наголошує на «суб'єктах», а не на створенні будь-якої цілісної системи стосовно того, як забезпечити базові потреби суспільства. **Завдання 3**. Ми також зазначили, що нова Директива CER значно розширить кількість секторів КІ, які потенційно будуть розглядатися як європейська, що підлягає не лише національному, а й зростаючому наднаціональному моніторингу та регулюванню. Крім того, директива також запроваджує системний рівень КІ через залежності та взаємозалежності між установами, секторами та країнами. Однак саме по собі це поняття не дає інструментів для розуміння конкретних залежностей і взаємозалежностей, а також того, як з ними боротися. Це, очевидно, дає багато можливостей для спекулятивного регулювання. **Завдання 4.** У новій Директиві CER ландшафт ризиків розширено, особливо за рахунок розгляду фізичних і цифрових ризиків як більш взаємопов'язаних порівняно з попередньою директивою; це також вносить у картину складність гібридних загроз. Ми зазначили, що будь-якій одній «критично важливій організації» може бути важко захиститися від таких гібридних загроз у межах своїх звичайних повноважень. Очевидно, що на національному рівні та на рівні ЄС знадобляться набагато більш скоординовані міжсекторальні мережі між різними органами влади, операторами КІ та іншими зацікавленими сторонами. Виклик 5. Крім того, проблема впливу Директиви CER досягає кульмінації в її посиленні регуляторних повноважень не лише над державами-членами, але й над окремими об'єктами CI або CE. Незважаючи на те, що прямі повноваження передані державам-членам, здається очевидним, що Європейська комісія може вжити заходів, принаймні, якщо вона виявить певний ЄКІ «європейського значення», який падає нижче прийнятного рівня стійкості, навіть якщо немає спільно узгоджених - за критеріями або стандартами. Виклик 6. Хоча підхід і цілі Директиви CER можна захистити, і ми всі за це в принципі, найближчі роки будуть свідчити про деякі проблеми щодо здатності цієї Директиви безперебійно працювати для досягнення своїх цілей. Основний негативний потенціал полягає в тому, що імплементація директиви в її різних сферах може розвиватися в кількох напрямках залежно від підходів конкретної країни-члена. Це не сприяло б розвитку внутрішнього (єдиного) ринку на справедливій основі, але було б вигідно для держав-членів, які тлумачать директиву якомога вільніше (дешевше). Виклик 7. ЄС почав розробляти свою політику КІ на початку 2000-х років, багато в чому запозичуючи концепції та підходи у США, які почали розробляти свою політику дещо раніше. З роками здається, що ЄС став більш самостійними у визначенні та розробці своїх підходів. Це можна побачити, наприклад, у словниковому запасі. Проте прийняття концепції стійкості КІ є досить спільною точкою зору серед розвинутих ринкових економік. Те саме стосується таких

СТАЛА ТА СТІЙКА
ІНФРАСТРУКТУРА 2023, VOL. 8,NO. S1,
85-101
https://doi.org/10.1080/23789689.2022.2128562

викликів, як зростання складності та взаємозалежності, а також «нових» загроз і нових технологій. Тому важливо, щоб існували та будуть існувати платформи, як політичні, так і наукові, а також пов'язані зі стандартизацією питань, які підтримують міжнародний діалог з країнами-однодумцями. Підсумовуючи, ми робимо висновок, що нова Директива CER свідчить про посилення регулювання сектору КІ, як розширюючи, так і поглиблюючи наднаціональні тенденції в цій сфері. Це, швидше за все, також відображає загальний напрям європейської інтеграції з функціональної або експертної точки зору. Якщо підхід CER досягне більшості своїх цілей, Європейський Союз буде більш інтегрований у свою політику КІ та відповідні картини загроз, ніж раніше. Це означало б, що країни-члени та європейські громадяни вимагатимуть ще більш скоординованих рішень на європейському рівні замість індивідуальної політики держав-членів, особливо під час криз.

Заява про розкриття інформації

Коаліція за стійку до стихійних лих інфраструктуру (CDRI) переглянула анонімну анотацію статті, але не брала участі в процесі експертної перевірки та остаточному редакційному рішенні. Фінансування публікації статті (APC) для цієї статті фінансується Коаліцією за стійку до стихійних лих інфраструктуру (CDRI). Примітки щодо авторів. Крістер Пурсіайнен є професором соціальної безпеки та безпеки на кафедрі технології та безпеки факультету науки та технологій Арктичного університету Норвегії (UiT) у Тромсе, Норвегія, з 2014 року. Він захистив докторську дисертацію з політичних наук /Міжнародні відносини в Університеті Гельсінкі в 1999 році. Раніше Пурсіяйнен працював на провідних керівних і дослідницьких посадах у таких установах, як Спільний дослідницький центр Європейської Комісії, JRC, Інститут захисту та безпеки громадян (Італія, Іспра); Рада держав Балтійського моря, СГБМ (Швеція, Стокгольм); Nordregio, Північний центр просторового розвитку (Швеція, Стокгольм); Російсько-Європейський центр економічної політики РЕЦЕП (Російська Федерація, Москва); Aleksanteri Institute – Фінський центр російських та східноєвропейських досліджень при Гельсінському університеті; та Фінського інституту міжнародних відносин UPI-FIIA (Фінляндія, Гельсінкі). Його публікації складаються з близько ста тридцяти наукових публікацій на різноманітні теми, включаючи безпеку суспільства, управління кризами, захист критичної інфраструктури та її стійкість, аналіз зовнішньої політики, а також регіональне співробітництво та інтеграцію. Ееро Кітомаа працює радником міністра в підрозділі національної безпеки Міністерства внутрішніх справ Фінляндії. Він багато працював над протидією гібридним загрозам і плануванням політики стійкості у Фінляндії та в ЄС і НАТО. В останні роки Kytömaa представляв Фінляндію на переговорах Європейської Ради щодо Директиви щодо стійкості критичних об'єктів. У 2016-2019 рр. пан Кітомаа працював у штаб-квартирі НАТО з питань оборонної політики та планування 97 відділу підтримки та стійкості, на посаді штабного офіцера з питань стійкості (VNC). Серед інших обов'язків Kytömaa координував роботу групи планування IRCSG, яка розглядала такі питання, як оперативні вказівки щодо пріоритетного доступу, моделювання стійкості до зрілості та енергетичні взаємозалежності. Крім того, він брав участь у напрямках роботи, пов'язаних з безпекою регіону Балтійського моря. До того, як приєднатися до державного сектору, пан Кітомаа працював в організації Crisis Management Initiative (CMI), яку заснував лауреат Нобелівської премії миру та колишній президент Фінляндії Мартті Ахтісаарі. Його публікації складаються зі статей про національну безпеку, протидію гібридним загрозам та стійкість.